

УДК 621.391.82

**МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ ВИДЕОИНФОРМАЦИИ
ШИМ-ПРЕОБРАЗОВАТЕЛЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ**

*д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК, С.В. ХАРЧЕНКО
(Полоцкий государственный университет)*

Разработана методика оценки защищенности видеоинформации ШИМ-преобразователя средств вычислительной техники (СВТ). Разработана экспериментальная модель исследования каналов утечки видеоинформации ШИМ-преобразователя СВТ. Принятие решения о защищенности основано на сравнении нормативного значения отношения мощности сигнала к мощности шума полученного результата с тестовым информационным сигналом. Методика позволяет получить результаты оценки защищенности ШИМ-преобразователя с высокой избирательностью, исключая влияющие факторы от других источников информации СВТ. Методика устанавливает требования по защите каналов утечки видеоинформации с использованием модели исследования ШИМ-преобразователя СВТ.

Ключевые слова: защита информации, широтно-импульсная модуляция, каналы утечки информации, побочные электромагнитные излучения и наводки.

Защита информации от утечки по техническим каналам сформировалась как составная часть противодействия мониторингу, в большей степени техническим компонентам. Очевидно, что основные требования к противодействию мониторингу (скрытность, маскировка, дезинформация, своевременность, непрерывность, правдоподобность) присущи мероприятиям по защите информации. Практически все научные исследования и разработки, а также меры по противодействию мониторингу учитывали вопросы защиты информации, включали это направление либо как основной элемент, либо как одну из важных частей исследований и разработок. Естественно, что научно-технические достижения, полученные в области противодействия техническим видам мониторинга, использовались и используются для целей защиты информации [1].

При выявлении технических каналов утечки информации, средства вычислительной техники рассматривают как систему, включающую:

- основное (стационарное) оборудование;
- оконечные устройства;
- соединительные линии;
- систему заземления;
- вспомогательные технические средства и системы, которые находятся в одном помещении с основными техническими средствами;
- технические средства открытой телефонной, громкоговорящей связи;
- системы охранной и пожарной сигнализации;
- электробытовые приборы и т.д. [2].

Наибольший интерес представляют вспомогательные технические средства и системы, имеющие выход за пределы контролируемой зоны, посторонние провода и кабели, к ним не относящиеся, но проходящие через помещение, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

В зависимости от физической природы возникновения информационных сигналов, среды их распространения и способов перехвата технические каналы утечки информации можно разделить на электромагнитные и электрические.

Электромагнитные каналы утечки информации. К электромагнитным относятся каналы утечки информации, возникающие за счет побочных электромагнитных излучений различного вида:

- излучений элементов СВТ (носителем информации является электрический ток, сила, напряжение, частота или фаза которого изменяется по закону информационного сигнала);
- излучений на частотах работы высокочастотных генераторов СВТ (устройства – задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.);
- излучений на частотах самовозбуждения усилителей низкой частоты СВТ (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Самовозбуждение наблюдается при переводе усилителя низкой частоты в режим перегрузки) [2].

Электрические каналы утечки информации. Электрические каналы утечки информации возникают за счет:

- наводок электромагнитных излучений СВТ на вспомогательные технические средства и системы и их соединительные линии, выходящие за пределы контролируемой зоны;
- просачивания электромагнитных сигналов в цепи электропитания (возможны при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, что обуславливает изменение потребляемого тока по закону изменения информационного сигнала);
- просачивания информационных сигналов в цепи заземления (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны).

Побочные электромагнитные излучения и наводки (ПЭМИН) – это вид электромагнитных волн, возникающих в результате работы электрических приборов, в частности, протекания электрического тока по проводникам. Так как электромагнитные излучения есть возмущения электромагнитного поля, то при передаче информации через локальную сеть или на монитор посредством кабелей возникают электромагнитные излучения, которые при попадании на проводник (антенну считывающего устройства) порождают в нем ток, схожий с оригиналом. После дискретизации считанного сигнала можно восстановить данные, передаваемые через проводник, что может привести к утечке информации. Самым простым примером является устройство перехвата или радиоприемник, установленный на нужную частоту, с помощью которого можно перехватить информацию. Однако эти излучения имеют свойство затухать при удалении от источника излучения и маскироваться электромагнитным фоном. Опасность данного канала утечки информации заключается в том, что могут существовать условия для считывания побочных электромагнитных излучений с достаточным соотношением сигнал/шум. Однако сигнал может не только напрямую излучаться различными проводниками, по которым непосредственно передается информация, электромагнитные излучения наводятся на различные электропроводные материалы. Канал утечки информации ПЭМИН является пассивным, если не содержит излучатели. Это указывает на то, что обнаружить утечку через такой канал информации довольно сложно.

Помехи можно разделить на две категории – узкополосные и широкополосные. В узкополосной помехе (например, гармонической) мощность сконцентрирована в узкой полосе частот. На практике в подавляющем большинстве случаев помеха имеет явно выраженный широкополосный, импульсный характер. Чем короче импульс (или длительность скачка напряжения) по сравнению с периодом его повторения, тем, в соответствии с Фурье-распределением, более широкополосная помеха и тем большее количество гармоник может излучаться.

В современных радиотехнических устройствах используются импульсы с очень острыми фронтами, что еще в большей степени увеличивает потенциальное количество существующих гармоник от таких источников помех. В любом случае импульсная последовательность возбуждает сильное переменное магнитное поле, легко проникающее в другие цепи, особенно на высоких частотах.

Широтно-импульсная модуляция (ШИМ) – это способ рационального управления подачей мощности к нагрузке. Управление заключается в изменении длительности импульсов при постоянной частоте их следования. Широтно-импульсная модуляция бывает различных видов.

Основной причиной применения ШИМ является стремление к повышению КПД при построении вторичных источников питания электронной аппаратуры.

Целью данной статьи является разработка и обоснование методики оценки защищенности видеoinформации СВТ, питаемого ШИМ-преобразователем.

Для реализации поставленной цели необходимо решить следующие задачи:

1. Разработать экспериментальную модель для исследования каналов утечки ШИМ-преобразователя СВТ.
2. Предложить тестовые сигналы и критерий оценки защищенности видеoinформации ШИМ-преобразователя СВТ.
3. Исследовать и обосновать алгоритм разработанной методики оценки защищенности ШИМ-преобразователя СВТ.

Особенности возникновения и распространения электромагнитной помехи

Поля ближней, дальней и промежуточной зон. Как известно из теории электромагнитных волн, электрическая и магнитная составляющие переменного во времени поля, связанные соответственно с напряжением и током, существуют одновременно в любой простейшей цепи переменного тока. Одна из составляющих поля, однако, может быть намного больше другой.

Характеристики поля в сильной степени зависят от расстояния до воспринимающего устройства, от параметров излучателя, параметров среды распространения и других факторов.

Как правило, расстояние до излучателя оценивают в относительных единицах R , связанных с длиной волны излучаемой помехи:

$$R = \lambda / 2\pi .$$

В соответствии с этим пространство вокруг источника делится на три зоны:

- ближнюю (поле индукции), в которой $R < 1$;
- дальнюю (поле плоской волны), в которой $R > 2$;
- промежуточную, когда $1 < R < 2$.

В зависимости от параметров источника помех ближняя зона может представлять собой или преимущественно поле магнитной индукции H , когда в источнике протекает значительный ток при относительно малых напряжениях, или преимущественно поле электрической индукции E , когда в источнике протекают малые токи при больших напряжениях. При этом в ближней зоне E и H находятся в фазе и сдвинуты в пространстве на 90 градусов.

По отношению к сопротивлению свободного пространства $Z_в$ поле E – высокоимпедансное, а поле H – низкоимпедансное.

Для высокоимпедансного поля (в ближней зоне):

- составляющая E убывает с расстоянием в кубе;
- составляющая H убывает с расстоянием в квадрате.

Для низкоимпедансного поля (в ближней зоне):

- составляющая H убывает с расстоянием в кубе;
- составляющая E убывает с расстоянием в квадрате.

При этом предполагается, что размеры излучателя во много раз меньше длины волны. В промежуточной зоне все составляющие поля убывают с расстоянием в квадрате, а в дальней зоне все составляющие поля убывают с расстоянием линейно.

Особенности учета электрических помех. Электрическая связь между цепями возникает из-за наличия емкостных паразитных связей между этими цепями. Для уменьшения наведенного паразитного напряжения следует уменьшать емкость связи и снижать сопротивление нагрузки в цепи наведенного напряжения по переменному току.

Для уменьшения паразитных связей используют экраны. Для того чтобы экран выполнял свои функции на высокой частоте, комплексное сопротивление самого экрана или заземляющего проводника должно быть меньше сопротивления емкости между экраном и источником паразитного излучения. Соответственно, экран должен иметь достаточно качественный контакт с корпусом в рабочем диапазоне частот.

Защита магнитных полей. Магнитные поля возникают вокруг токоведущих проводников, высокочастотных катушек индуктивности, дросселей и трансформаторов. Передача магнитной энергии происходит посредством взаимоиндукции, существующей между цепями. Как известно, ток, протекающий по проводнику одной цепи, вызывает магнитный поток, который наводит напряжение в другой цепи.

Экранирование аппаратуры от воздействия магнитных полей – дорогая и на низких частотах не всегда эффективная мера. На более высоких частотах современные экранирующие материалы обеспечивают более чем достаточное для большинства практических случаев затухание магнитных полей. Возникающие здесь проблемы связаны в основном с прохождением паразитных колебаний через неоднородности экранов (отверстия, щели и т.д.) и межмонтажными наводками.

Наиболее часто встречающимися источниками магнитного поля являются проводники, по которым протекают токи высокой частоты.

Защита от электромагнитного поля. Защита от электромагнитного поля – это защита от электромагнитных полей в дальней зоне. Сопротивление электромагнитной волны для дальней зоны одинаково для всех волн и равно сопротивлению свободного пространства. Напряженность поля с расстоянием уменьшается линейно. Основным способом защиты от электромагнитных помех в этой зоне – экранирование и уменьшение мощности помех в самом источнике.

Обычно, если экран хорошо выполняет возложенную на него задачу в ближних полях, то экранирование оказывается достаточным и для полей дальней зоны.

Разработка экспериментальной модели для исследования каналов утечки видеoinформации ШИМ-преобразователя питания. Блок-схема разработанной экспериментальной модели для исследования каналов утечки информации изображена на рисунке 1.

Экспериментальная модель состоит из следующих компонентов:

- ШИМ-преобразователь питания. В качестве объекта испытаний используется преобразователь питания видеомонитора, преобразующий переменный ток сети напряжением 220 В в постоянный ток напряжением 12 В;
- монитор LG 786LS (служит нагрузкой преобразователя питания);
- ПЭВМ (источник видеoinформации, передаваемой на видеомонитор посредством кабеля интерфейса VGA);
- анализатор спектра;
- эквивалент сети.

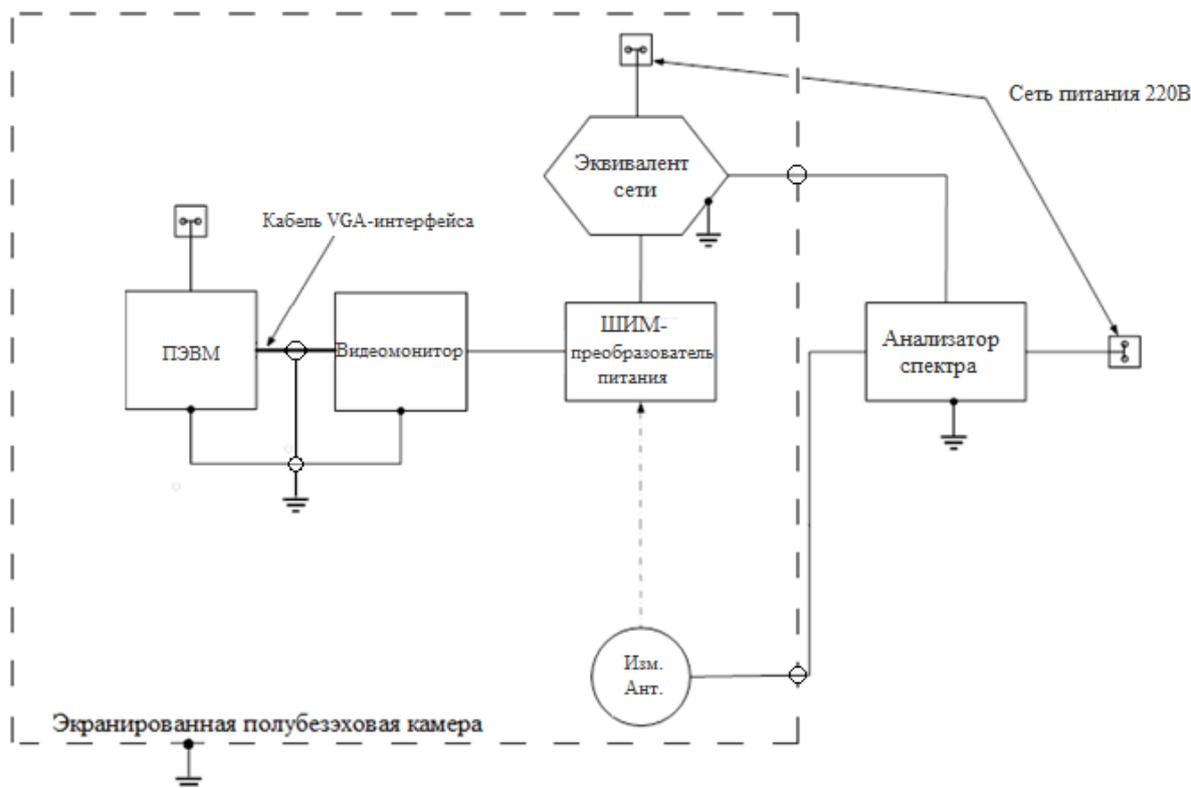


Рисунок 1. – Блок-схема экспериментальной модели для исследования каналов утечки видеoinформации ШИМ-преобразователя питания СВТ

Для увеличения достоверности результатов применялись пассивные методы снижения электромагнитных излучений: экранирование и заземление видеомонитора, ПЭВМ, соединительных линий. Измерительное оборудование, а также экранированная полубезэховая камера имеют соответствующие свидетельства о калибровке и аттестат. Измерения проводились в соответствии с ГОСТ Р 51320-99, что повышает достоверность оценки параметров информативных каналов утечки. Модель учитывает требования стандартов, вследствие чего снижается влияние промышленных помех высокого уровня.

Тестовые сигналы и критерий оценки защищенности видеoinформации ШИМ-преобразователя СВТ. В методике предложен тестовый информационный сигнал, параметры которого соответствуют однополярной меандровой последовательности, соответствующей параметрам последовательности элементарных посылок видеосигнала. В этом режиме длительности соответствующих импульсов и пауз между ними равны $T_u / \tau_u = 2$.

В зависимости от установленного видеоразрешения число строк в кадре и число пикселей в строке есть стандартные числа. Методика предусматривает использование видеомониторов с различной разрешающей способностью, которая влияет на значение тактовой частоты тестового измерительного сигнала.

Используемый в исследовании видеомонитор работает с разрешающей способностью $1024 \times 768 \times 60$ Гц. Это значит, что в одной строке формируется 512 «черных» и 512 «белых» пикселей, таких строк в кадре 768 при 60 кадрах в секунду.

Из вышеприведенного следует, что формируется сигнал в виде пакета из 512 импульсов, затем имеют место некая пауза на обратный ход в начало строки и новая строка. И так 768 строк. После этого следует более длительная пауза на обратный ход в начало следующего кадра. И так 60 раз в секунду. Из этого рассчитаем тактовую частоту тестового сигнала. Проходят 512 импульсов в 762 строках с обновлением 60 Гц; учитывая частоту обратного хода, получаем $512762 \cdot 60 \cdot 1,37 \approx 32,4$ МГц. Таким образом, была вычислена тактовая частота информационного измерительного тестового сигнала.

На рисунке 2 схематически представлен спектральный состав тестового измерительного сигнала, из которого следует наличие информативных гармоник, соответствующих меандровому сигналу с представленными параметрами.

Критерием оценки защищенности будем считать отношение напряженности гармонических составляющих тестового измерительного сигнала к напряженности опорного сигнала, в качестве которого используется сигнал «белое поле».

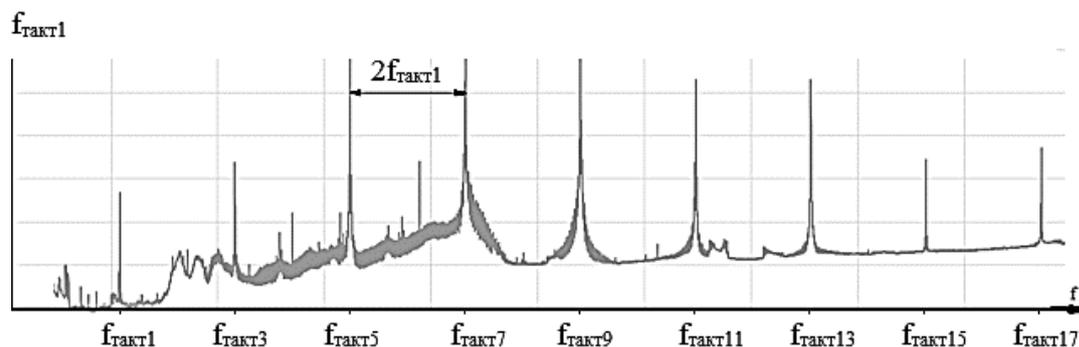


Рисунок 2. – График спектральной плотности тестового сигнала

Алгоритм оценки защищенности видеoinформации ШИМ-преобразователя:

- экспериментальная модель приводится в рабочий режим;
- на ПЭВМ формируется опорный сигнал «белое поле», который посредством VGA интерфейса подается на видеомонитор;
- при помощи измерительного оборудования производится замер фоновой обстановки;
- на ПЭВМ формируется информационный сигнал «точка через точку», который посредством VGA интерфейса подается на видеомонитор;
- производится повторный замер фоновой обстановки;
- при помощи анализатора спектра оба замера сравниваются, и производится поиск информационного сигнала.

Преимущественно поиск производится на частоте 32,4 МГц и ее нечетных гармониках. Чтобы убедиться в информативности найденного сигнала, достаточно, настроившись на его частоту, изменить исходный тест на ПЭВМ – вместо сигнала «точка через точку» установить зеленое, красное либо синее поле. В этом случае найденный сигнал должен изменять форму импульсов в зависимости от исходного сигнала, сохраняя параметры несущей. Если указанные условия выполняются, то считаем найденный сигнал информационным.

Исследование разработанной экспериментальной модели на наличие каналов утечки видеoinформации по сети питания. Измерения производились при подключении ШИМ-преобразователя питания через эквивалент сети. Поиск информационных сигналов производился в разных полосах пропускания приемника и в диапазоне частот 0,15–1000 МГц. Для наглядности в статье представлены данные в диапазоне 30–500 МГц, так как информационных сигналов на более высоких частотах обнаружить не удалось. Необходимо учесть, что из-за неэкранированного источника питания, соединительных кабелей и отсутствия сетевого фильтра в сеть питания утекает большое количество посторонних помех. Измеренные спектры гармоник информационного сигнала показаны на рисунке 3. Найденные информационные сигналы представлены в таблице 1.

Таблица 1

№ гармоники информационного сигнала	Частота, МГц	$E_{инф}$, дБ мкВ/м
5	162,01	22,51
7	226,81	7,29
9	291,61	5,63
11	356,41	6,38
13	421,21	5,33

На основании полученных результатов можно сделать вывод, что утечка информации в сеть питания может происходить по следующим причинам:

- наводки ПЭМИН на неэкранированный кабель, а именно кабель сети питания и кабель, соединяющий ШИМ-преобразователь питания и монитор;
- плохое исполнение сетевого фильтра в ШИМ-преобразователе питания.

Исследование разработанной экспериментальной модели на наличие каналов утечки видеoinформации в эфир. Поиск информационных сигналов производился в горизонтальной и вертикальной поляризациях измерительной антенны в диапазоне 30–1000 МГц.

Измеренные спектры гармоник информационного сигнала показаны на рисунке 4.

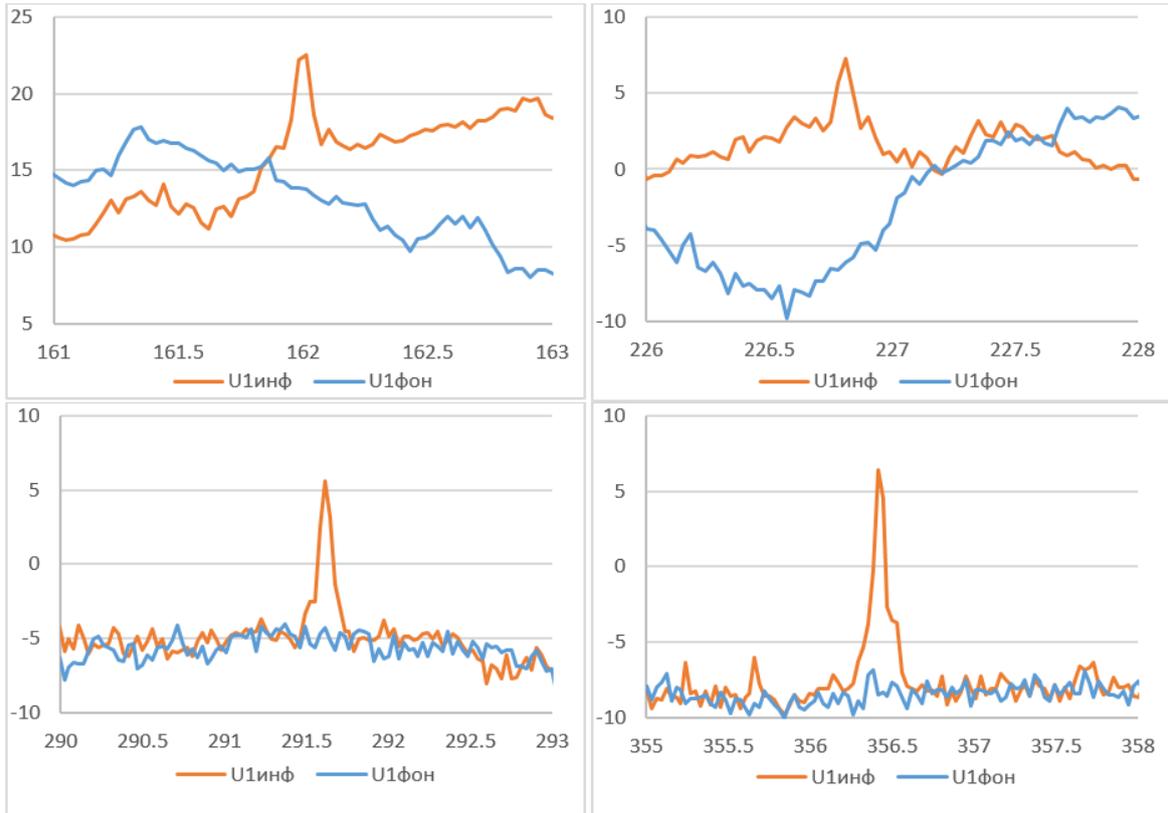


Рисунок 3. – Спектры 5-й, 7-й, 9-й и 11-й гармоник

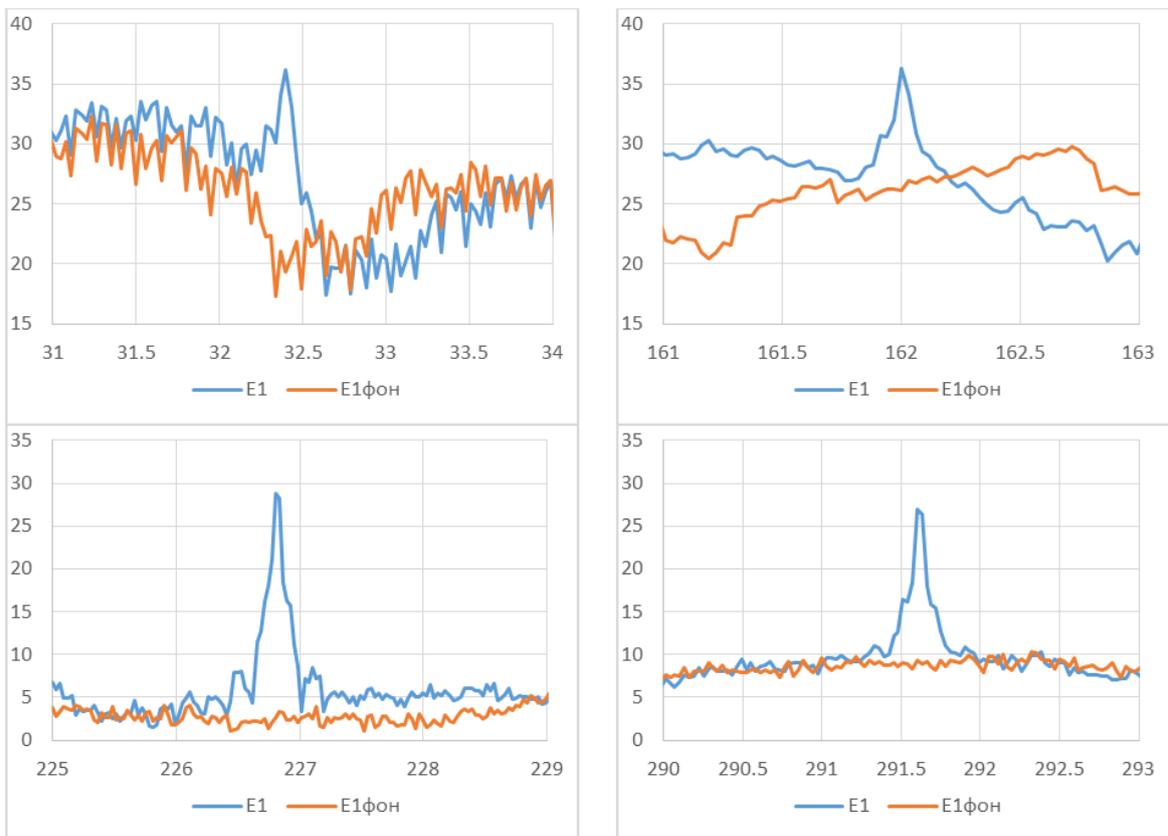


Рисунок 4. – Спектры 1-й, 5-й, 7-й и 9-ой гармоник

В результате измерений при помощи антенны СВЛ экспериментальным путем были найдены информационные сигналы, их частоты и уровни напряженности (таблица 2).

Таблица 2

№ гармоники информационного сигнала	Частота, МГц	$E_{инф}$, дБ мкВ/м
1	32,4	36,2
5	162,1	36,3
7	226,8	28,2
9	291,6	26,4
11	356,4	26,4
15	486,0	24,9
17	550,8	26,8
19	615,6	23,6

Из полученных результатов можно сделать вывод, что утечка информации в эфир может происходить из-за отсутствия экранирования ШИМ-преобразователя питания, а также соединительных кабелей.

Необходимо учесть, что из-за неэкранированного источника питания и неэкранированных соединительных кабелей в эфир утекает большое количество промышленных помех, которые могут плохо сказываться на работу другого оборудования.

Возможные пассивные методы подавления промышленных помех:

1. *Фильтрация.* Этот метод является основным средством ослабления кондуктивных помех, создаваемых в цепях питания и коммутации постоянного и переменного токов аппаратуры. Ослабление помех с помощью фильтрации достигается:

- шунтированием их на землю;
- отражением их обратно к источнику;
- рассеиванием (превращением их энергии в тепловую).

2. *Заземление.* Наряду с известными функциями защиты и безопасности заземляющая система должна:

- представлять собой цепь опорного источника напряжения;
- обеспечивать сигнальные и силовые цепи возврата;
- препятствовать появлению вблизи антенн высокочастотных потенциалов и свести к минимуму нежелательные паразитные связи между сигналами.

Протекание токов в системе заземления приводит к разности потенциалов, которая для обеспечения нормальной работы оборудования должна быть невелика по сравнению с амплитудой сигнала. Поэтому при проектировании системы заземления следует поддерживать импеданс заземления на как можно более низком уровне.

3. *Экранирование.* В большинстве практических случаев для защиты от помех и наводок достаточно эффективности экранирования в 30–60 дБ и лишь в некоторых ответственных местах (кухонь передатчика, источника питания, экран интерфейсного кабеля и др.) требуется величина затухания на уровне 50–100 дБ. На частотах выше 100 кГц однослойные экраны обеспечивают эффективность экранирования 40–70 дБ, а двухслойные – до 120 дБ. Отверстия и зазоры ограничивают ослабление электрических и высокочастотных полей, в то время как ослабление низкочастотных магнитных полей определяется материалом экрана и его толщиной. При этом, естественно, следует учитывать, что материал не должен насыщаться.

Заключение. Проанализированы возможные каналы утечки информации ШИМ-преобразователя питания СВТ. Разработана методика оценки защищенности видеoinформации ШИМ-преобразователя СВТ.

На основании разработанной методики проведена оценка защищенности видеoinформации ШИМ-преобразователя СВТ; исследования каналов утечки видеoinформации производились в двух средах распространения:

- излучение информационного сигнала в цепь питания в виде кондуктивных помех;
- излучение информационного сигнала в эфир в виде электромагнитных излучений.

В результате проведения измерений были обнаружены излучения информационного сигнала «точка через точку» превышали уровень излучения опорного (фоновое) сигнала «белое поле» в среднем на ~10 дБ мкВ. В эфире уровни излучения информационного сигнала «точка через точку» превышали уровни опорного (фоновое) сигнала «белое поле» в среднем на ~20 дБ мкВ.

ЛИТЕРАТУРА

1. Железняк, В.К. Защита информации от утечки по техническим каналам : учеб. пособие / В.К. Железняк. – СПб., ГУАП. – 2006. – 188 с.

2. Хорев, А.А. Защита информации от утечки по техническим каналам : учеб. пособие / А.А. Хорев. – М. : Гостехкомиссия РФ, 1998. – Ч. 1 : Технические каналы утечки информации. – 320 с.
3. Сергиенко, А.Б. Цифровая обработка сигналов : учеб. для вузов / А.Б. Сергиенко. – СПб. : Питер, 2002. – 608 с.
4. Кашкаров, А.П. Импульсные источники питания: схемотехника и ремонт / А.П. Кашкаров. – М. : ДМК Пресс, 2012. – 184 с.
5. Уайт, Д. Электромагнитная совместимость и непреднамеренные помехи : в 3-х вып. / Д. Уайт. – М. : Советское радио, 1977. – 352 с.
6. Князев, А.Д. Элементы теории и практики обеспечения электромагнитной совместимости радиоэлектронных средств / А.Д. Князев. – М. : Радио и связь, 1984. – 336 с.
7. Полонский, Н.В. Конструирование электромагнитных экранов для РЭА / Н.В. Полонский. – М. : Советское радио, 1979. – 216 с.
8. Вайнштейн, Л.А. Электромагнитные волны / Л.А. Вайнштейн. – М. : Радио и связь, 1988. – 440 с.

Поступила 11.03.2020

METHODOLOGY FOR ESTIMATING VIDEO INFORMATION SECURITY OF PWM CONVERTER OF COMPUTER EQUIPMENT

V. ZHELEZNYAK, S. HARCHENKO

Designed by methodology for assessing the security of video information of a PWM converter of computer equipment. A technique for assessing the security of video information of a PWM converter of computer equipment is considered. An experimental model for the study of leakage channels of video information of a PWM converter of computer technology has been developed. The adoption of a security permission is based on a comparison of the normative value of the ratio of signal power to noise power of the obtained result using a test information signal. The technique allows to obtain the results of assessing the security of a PWM converter with high selectivity, excluding influencing factors from other information sources of computer equipment. The methodology establishes requirements for the protection of video leakage channels using a research model of a PWM converter of computer equipment.

Keywords: *information protection, pulse width modulation, information leakage channels, Transient Electromagnetic Pulse Emanation Standard.*